Understanding and Responding to Distributed Denial-of-Service Attacks

Denial-of-service (DoS) attacks aim to overwhelm a specific application or website, draining the system's resources and making it unavailable to legitimate users. There are several types of DoS attacks:

- **Network Resource Overload**: This involves exhausting all available network capacities of the target, either through:
  - Direct attacks like exploiting server weaknesses or flooding servers with excessive requests.
  - Reflection amplification attacks, where the attacker uses a third-party server to redirect a large amount of traffic to the target, using spoofed IP addresses.
- **Protocol Resource Overload**: Targets the session or connection capacities of the system.
- **Application Resource Overload**: Focuses on using up the target's computing or storage capabilities.

A DDoS attack isn't solely about overwhelming volume; it can also target specific aspects of a network or application to exhaust resources. Such attacks may focus on exploiting vulnerabilities in protocols or applications, causing disruption without necessarily generating high traffic volumes.

The effectiveness of a DDoS (Distributed Denial of Service) attack escalates with the amount of generated traffic, complicating an organization's response and recovery efforts.

This increased traffic can obscure the attack's origin, making attribution difficult. While some DDoS attacks might have minimal impact, others can cause significant issues, including disruption of crucial services, loss of productivity, high recovery costs, and serious damage to reputation. To mitigate these risks, organizations should integrate specific strategies into their incident response and business continuity plans. Importantly, while DDoS attacks typically don't compromise data confidentiality or integrity, they significantly hinder system availability and legitimate usage.

Recommendations

- Identify and prioritize your critical assets and services. Determine which services are accessible via the public internet and understand their vulnerabilities. Rank these assets based on their importance to your mission and their necessity for continuous availability.
- Grasp the methods by which your users access your network. Assess the various ways they connect, whether it's directly on-site or remotely through virtual private networks (VPNs). Look for potential bottlenecks in the network and find solutions that can help reduce disruption for essential personnel.
- Consider subscribing to a specialized DDoS protection service. While many internet service providers offer basic DDoS defenses, a service dedicated to DDoS protection might offer more comprehensive safeguards, particularly against larger or more sophisticated attacks.
- Learn about the DDoS defense strategies of your Internet Service Provider (ISP) and Cloud Service Provider (CSP). Discuss with them the specifics of their DDoS protection and review your service agreements to understand the extent of assistance they offer against DDoS attacks. Also, evaluate any potential risks due to coverage limitations. Consult with your service providers for optimal practices in hosting web servers under their DDoS protection framework.
- Geofencing can be an effective defense strategy when your target audience is confined to a specific region. By setting up a virtual geographic boundary, geofencing allows you to restrict access to your services based on location. This means anyone attempting to access your services from outside the predefined area could be automatically blocked, reducing the risk of certain types of cyber attacks, like Distributed Denial of Service (DDoS), especially if the threat is known to originate from regions outside your audience's location. This localized approach to cybersecurity can be a key component in safeguarding your digital assets.
  - If you're looking to create a geofencing list for your routers or network devices, there's an open-source tool available that can facilitate this process. This tool offers a practical and cost-effective way to enhance your network's security by defining geographical boundaries.

Detection and Incident Response

- Collecting evidence during a DDoS attack is crucial, even though it may seem overwhelming in the moment. This evidence can provide valuable insights into the attack's patterns and origins. By analyzing this data, you can identify vulnerabilities, improve your defensive strategies, and possibly assist in legal actions against the attackers. Moreover, understanding the nature of the attack can help in developing more robust protection mechanisms and in preparing better for future incidents. Always remember, every bit of information counts in enhancing your cyber resilience.
- Network packet capture is a valuable tool in cybersecurity, particularly in the context of understanding and mitigating attacks. By recording all the packets passing through a network, it allows for a detailed examination of the traffic, which can be crucial in identifying the nature and source of cyber threats like DDoS attacks. This data can provide insights into attack patterns, helping in enhancing network defenses. Additionally, captured packet data can serve as evidence for forensic analysis and legal proceedings related to cyber attacks. Essentially, packet capture acts as a comprehensive record of network activity, making it a key component in both immediate response and long-term security strategy. Don't hesitate to send pcap files to CIRCL for further analysis.

References

- CISA - Understanding and Responding to Distributed Denial-of-Service Attacks
- Open Source Tool to create geolist of IP CIDR blocks - https://github.com/gallypette/blocknolu

Classification of this document

TLP:CLEAR information may be distributed without restriction, subject to copyright controls.

Revision

- Version 1.0 - TLP:CLEAR - First version - 9th February 2024

Understanding and Responding to Distributed Denial-of-Service Attacks

↑ Back to Publications and Presentations

Recommendations

Detection and Incident Response

References

Classification of this document

Revision

You can report incidents via our official contact including e-mail, phone or use the Anonymous reporting form.

Search

CIRCL is the CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.
Content from this website is classified as TLP:CLEAR (previously: TLP:WHITE) information may be distributed without restriction, subject to copyright controls.
Copyright 2008 - 2023 CIRCL Computer Incident Response Center Luxembourg (LHC - Luxembourg House of Cybersecurity).
PGP signature of this page and How to Verify Integrity of CIRCL Web Pages

Mastodon